CLAIMS:

1. A method for detecting modifications to code placed in memory by the Power On Self Test (POST) Basic Input/Output System (BIOS) comprising the steps of:

initiating said POST operation;

retrieving code from a flash memory;

measuring said retrieved code to generate a first measurement;

storing said first measurement in a secure area;

storing said retrieved code in a memory located in a non-secure area;

measuring said retrieved code stored in said memory located in said non-secure area after receiving an awakening event to generate a second measurement; and

indicating said retrieved code stored in said memory was modified if said first measurement is not equal with said second measurement.

2. The method as recited in claim 1 further comprising the step of:

awakening a system if said first measurement is equal with said second measurement.

3. The method as recited in claim 1, wherein said indication comprises an error message.

4. The method as recited in claim 1 further comprising the step of:

rebooting a system thereby restoring said retrieved code to its proper values.

5. The method as recited in claim 1, wherein said retrieved code comprises one or more of the following: legacy BIOS code and code used to support said legacy BIOS code.

6. The method as recited in claim 5, wherein said code used to support said legacy BIOS code comprises one or more of the following: Universal Serial Bus (USB) interface support code and code for power management routines.

7. The method as recited in claim 1, wherein said secure area is located within a trusted building block of a system.

8. The method as recited in claim 1, wherein said secure area comprises a lockable Electrically Erasable Programmable Read Only Memory (EEPROM) module.

9. A computer program product embodied in a machine readable medium for detecting modifications to code placed in memory by the Power On Self Test (POST) Basic Input/Output System (BIOS) comprising the programming steps of:

initiating said POST operation;

retrieving code from a flash memory;

measuring said retrieved code to generate a first measurement;

storing said first measurement in a secure area;

storing said retrieved code in a memory located in a non-secure area;

measuring said retrieved code stored in said memory located in said non-secure area after receiving an awakening event to generate a second measurement; and

indicating said retrieved code stored in said memory was modified if said first measurement is not equal with said second measurement.

10. The computer program product as recited in claim 9 further comprising the programming step of:

awakening a system if said first measurement is equal with said second measurement.

11. The computer program product as recited in claim 9, wherein said indication comprises an error message.

12. The computer program product as recited in claim 9 further comprising the programming step of:

rebooting a system thereby restoring said retrieved code to its proper values.

13. The computer program product as recited in claim 9, wherein said retrieved code comprises one or more of the following: legacy BIOS code and code used to support said legacy BIOS code.

14. The computer program product as recited in claim 13, wherein said code used to support said legacy BIOS code comprises one or more of the following: Universal Serial Bus (USB) interface support code and code for power management routines.

15. The computer program product as recited in claim 9, wherein said secure area is located within a trusted building block of a system.

16. The method as recited in claim 9, wherein said secure area comprises a lockable Electrically Erasable Programmable Read Only Memory (EEPROM) module.

17. A system, comprising:

a memory;

a processor coupled to said memory;

a first portion of a flash memory coupled to said processor, wherein said first portion of said flash memory comprises a Power On Self Test (POST) Basic Input/Output System (BIOS) code; and

a Trusted Building Block (TBB) coupled to said processor, wherein said TBB is configured to ensure integrity of said system, wherein said TBB comprises:

a second portion of said flash memory, wherein said second portion of said flash memory in said TBB comprises:

a boot block code, wherein said boot block code comprises code to reset said system; and

code to be moved from said second portion of said flash memory to said memory by said POST BIOS code during a POST operation;

wherein said processor, responsive to said POST BIOS code, comprises:

circuitry operable for retrieving said code from said second portion of said flash memory during said POST operation;

circuitry operable for measuring said retrieved code to generate a first measurement;

circuitry operable for storing said first measurement in a secure area; and

circuitry operable for storing said retrieved code in said memory; and

wherein said processor, responsive to said boot block code, comprises:

circuitry operable for measuring said retrieved code stored in said memory after receiving an awakening event to generate a second measurement; and

circuitry operable for indicating said retrieved code stored in said memory was modified if said first measurement is not equal with said second measurement.

18. The system as recited in claim 17, wherein said processor, responsive to said boot block code, further comprises:

circuitry operable for awakening said system if said first measurement is equal with said second measurement.

19. The system as recited in claim 17, wherein said indication comprises an error message.

20. The system as recited in claim 17, wherein said processor, responsive to said boot block code, comprises:

circuitry operable for rebooting said system thereby restoring said retrieved code to its proper values if said first measurement is not equal with said second measurement.

21. The system as recited in claim 17, wherein said retrieved code comprises one or more of the following: legacy BIOS code and code used to support said legacy BIOS code.

22. The system as recited in claim 21, wherein said code used to support said legacy BIOS code comprises one or more of the following: Universal Serial Bus (USB) interface support code and code for power management routines.

23. The system as recited in claim 17, wherein said secure area is located within said TBB.

24. The system as recited in claim 17 further comprising:

a lockable Electrically Erasable Programmable Read Only Memory (EEPROM) module coupled to said processor, wherein said secure area comprises said lockable EEPROM module.